UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,423	10/31/2001	George S. Gales	10017055-1	2560

7590 09/22/2005	EXAMINER
HEWLETT-PACKARD COMPANY	SHERKAT, AREZOO
Intellectual Property Administration	

	ART UNIT	PAPER NUMBER
HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400	2131	

DATE MAILED: 09/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/002,423	GALES, GEORGE S.
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _28 June 2005_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-33_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-33_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment filed on June 28, 2005. Claims 1-33 are pending.

Response to Arguments

Applicant's arguments filed June 28, 2005 have been fully considered but they are not persuasive.

Examiner respectfully maintains the rejection formulated on March 18, 2005 as follows:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-33 are rejected under 35 U.S.C. 102(e) as being anticipated by

Rowland, (U.S. Patent No. 6,405,318).

Regarding claims 1 and 19, Rowland discloses a network intrusion

detection system, comprising:

a processor (i.e., local controller function 6), a memory accessible by the

processor (i.e., where log files are stored), a monitor application stored in the

memory and executable by the processor, the monitor application adapted to

monitor network activity associated with a network node (i.e., session monitoring

function 4), a profile application stored in the memory and executable by the

processor, the profile application adapted to automatically generate an activity

profile associated with the network node using the monitored network activity,

and a recognition engine stored in the memory and executable by the processor,

the recognition engine adapted to compare a network event to the activity profile

to determine whether the network event is authorized for the network node (i.e.,

log auditing function 10 monitors the system login auditing files 11 by comparing

the log file activity with known attack events 12, known security violations 13, and

events to ignore 14)(Col. 3, lines 30-67 and Col. 4, lines 1-48).

Regarding claims 2-4, Rowland discloses wherein the network activity

comprises inbound data communications and outbound data communications

(Col. 4, lines 30-48).

Regarding claim 5, Rowland discloses wherein the profile application generates the activity profile corresponding to network activity occurring over a predetermined time period (Col. 4, lines 15-30).

Regarding claims 6, 17, 26, and 28, Rowland discloses wherein the profile application is further adapted to automatically update the activity profile in response to a predetermined event (i.e., login events)(Col. 4, lines 30-48).

Regarding claims 7, 18, 25, 29, and 33, Rowland discloses wherein the profile application is further adapted to automatically update the activity profile corresponding to a predetermined time period (i.e., the log auditing function can run on a periodic basis with the period selected by the user or it can run continuously in real-time)(Col. 4, lines 30-48).

Regarding claims 8, 16, and 32, Rowland discloses wherein the recognition engine is further adapted to block the network event if the network event exceeds the activity profile (i.e., blocking access to the computer system)(Col. 6, lines 13-67 and Col. 7, lines 1-67 and Col. 8, lines 1-24).

Regarding claims 9, 15, and 20, Rowland discloses wherein the profile application is further adapted to automatically update the activity profile if the network event is authorized (i.e., if the user is logging into the system, the

monitor builds/updates the user profile database and updates the active user

database)(Col. 4, lines 30-48).

Regarding claims 10, 14, 22, and 30, Rowland discloses further

comprising an event library accessible by the recognition engine to determine

whether the network event is authorized, the event library comprising information

associated with authorized network activities not reflected in the activity profile

(Col. 7, lines 55-67 and Col. 8, lines 1-8).

Regarding claim 11, Rowland discloses a method for network intrusion

detection, comprising:

monitoring network activity associated with network node for

predetermined time period (i.e., session monitoring function 4 and port scan

detector function 5 all operate in real-time to detect an activity indicative of an

attack by unauthorized users or systems ... the log auditing function can run on a

periodic basis with the period selected by the user or it can run continuously in

real-time), automatically generating an activity profile corresponding to the

network node using the monitored network activity, identifying a network event

associated with the network node, and automatically determining whether the

network event is authorized for the network node using the activity profile (i.e.,

log auditin function 10 monitors the system login auditing files 11 by comparing

the log file activity with known attack events 12, known security violations 13, and

events to ignore 14. if the log file activity indicates a known attack event 12 or a

known security violation 13 indicating a suspicious event or unknown event has

occurred or is in the process of occuring, then the controller is informed to take

action)(Col. 4, lines 15-67 and Col. 5, lines 1-67 and Col. 6, lines 1-12).

Regarding claims 12, 21, and 31, Rowland discloses wherein monitoring

the network activity comprises monitoring the network activity comprising

inbound data communications and outbound data communications associated

with the network node (i.e., port scanning)(Col. 6, lines 13-67 and Col. 7, lines 1-

40).

Regarding claims 13 and 23, Rowland discloses wherein monitoring the

network activity comprises monitoring network application usage corresponding

to the network node (Col. 8, lines 46-67 and Col. 9, lines 1-52).

Regarding claim 24, Rowland discloses wherein the recognition engine is

further adapted to generate an event alarm log for the network event if the

network event is not authorized (Col. 8, lines 46-67 and Col. 9-10, lines 1-67 and

Col. 11, lines 1-42).

Regarding claim 27, Rowland discloses a computer program for assisting

in network intrusion detection, comprising;

a computer-readable medium, and a profile application stored on the

computer-readable medium, the profile application adapted to monitor network

activity and generate an activity profile using the monitored network activity, the activity profile used to determine whether a network event is authorized (i.e., log auditing function 10 monitors the system login auditing files 11 by comparing the log file activity with known attack events 12, known security violations 13, and events to ignore 14)(Col. 3, lines 30-67 and Col. 4, lines 1-48).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lermuzeaux et al., (U.S. Patent No. 5,621,889),

Milliken et al., (U.S. Publication No. 2004/0073617),

Epstein et al., (U.S. Patent No. 6,584,508),

Sheih et al., (U.S. Patent No. 5,278,901),

Milliken et al., (U.S. Publication No. 2004/0064737), and

Guheen et al., (U.S. Patent No. 6,473,794).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be
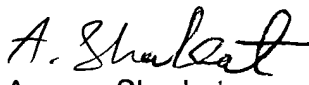
calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Arezoo Sherkat whose telephone number is

(571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-

Friday.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax

phone number for the organization where this application or proceeding is

assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free).

Arezoo Sherkat
Patent examiner
Group 2131
Sep. 19, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100